

PATENT APPLICATION
Docket No.: 5045.2.1D

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Vincent S. Darago and Christopher Jenkins
Serial No.: 10/609,325
Filed: June 27, 2003
For: Computer architecture for managing courseware in a
shared use operating environment
Art Unit: 2452
Examiner: Hieu T. Hoang

APPELLANT'S BRIEF

Honorable Commissioner for Patents:

In response to a Final Office Action mailed May 19, 2010 and pursuant to a Notice of Appeal filed September 17, 2010, and 37 C.F.R. §§ 41.30 *et seq.*, Assignee appeals to the Board for relief from decisions of the Examiner.

Real Party in Interest

The real party in interest in this appeal is Assignee, Digital-Vending Services International, LLC.

Related Appeals and Interferences

There are no pending related appeals or interferences. Patents related to the present application are in litigation, namely U.S. Patent Nos. 6170014, 6282573, and 6606664.

Status of Claims

Claims 131-155 are pending, are rejected, and are appealed.

Status of Amendments

No claim amendment was filed after final rejection.

Summary of Claimed Subject Matter

The claimed invention provides tools and techniques for managing courseware and other content in a shared use operating environment such as a computer network. (Abstract)

Courseware and other content managed by the system may contain one or more "critical portions" which have been treated to prevent their unauthorized use and thereby enhance the protection of intellectual property rights in the content by technical means. (Brief Summary)

Some embodiments provide the aspects noted below. Drawing reference numbers are given below in parentheses; paragraph numbers are given in square brackets [] and refer to the published application, US Pat. Pub. 20040073601:

131. (Figures 3-5, 7; published claims 16 and 23) A method for managing content in a shared use operating environment, the shared use operating environment including a registration server (108), a content server (110) connectable by a network link to the registration server, and a client workstation (114) connectable by a client-server network communications link to the content server, the method comprising the steps of:

registering [0126] (700), a user at the registration server, thereby characterizing the user as a registered user;

receiving at the content server a request (604) by the registered user for access to content (400) which contains at least one previously treated critical portion [0040];

authenticating [0039] (610) the request;

serving [0039] at least the critical portion over the client-server network communications link (116) for presentation to the registered user at the client workstation;

preventing [0040] a copy of the critical portion of the content from being created on nonvolatile storage [0058] at the client workstation at least in part by disabling caching and other disk writes, and

sending [0087] another portion of the content to nonvolatile storage at the client workstation.

132. (Figures 6 and 7) A method for managing content in an operating environment that includes peer-to-peer nodes [0061], the method comprising the steps of:

registering [0126] (700) users;

checking user passwords [0067, 0068, 0109] to prevent unregistered users from receiving content services;
receiving at a first peer node a request (604) by a registered user for access to content (400) which contains at least one previously treated critical portion [0040];
serving [0039] at least the critical portion over a network communications link (116) to a second peer node for presentation (712, 718, 720) to the registered user;
preventing [0040] a copy of the critical portion of the content from being created on nonvolatile storage [0058] at the second peer node, at least in part by disabling caching and other disk writes, and
sending [0087] another portion of the content to nonvolatile storage at the second peer node.

Note that the drawing reference numbers refer not only to the drawings but also to the specific locations in the text where the reference numbers are recited. The Office can readily determine those locations by searching a copy of the application. Also, the citations to drawings and text above are only examples; other parts of the specification may also be pertinent.

Grounds of Rejection to be Reviewed on Appeal

1. Claims 131, 132, 133, 140-145, 147-155 were rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser (US 6385596) in view of Benson (US 6678665) and assertions of Official Notice;
2. Claims 134-139, 146 were rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser, Benson, and Official Notice, and in view of Salesky (US 6343313).

Argument

Claim Grouping

The claims all belong to a single group, for purposes of the present appeal.

Ground 1 (Claims 131, 132, 133, 140-145, 147-155): “Portion” Means “Part”

The rejections err by relying on an unreasonable interpretation of the term “portion”. Contrary to the context in which “portion” is used in the specification and the claims, and contrary to the ordinary meaning of the term “portion”, the rejections confuse a “portion” of content with the whole content instead of recognizing that “portion” means “part”.

The claimed invention sends a critical portion of content only to volatile storage (by disabling caching and other disk writes for that portion) and sends another portion of the content to nonvolatile storage. Together, the “critical portion” and the “another portion” constitute the whole of the served content. Claims 131, 132.

At page 2 the Final Office Action asserts that this distinction was known because Wiser made it obvious to disable caching and writing of encrypted content and sent a preview portion of content which is allowed to be stored in nonvolatile storage. Thus, the rejections rely on an interpretation in which Wiser’s encrypted content corresponds to the present invention’s critical portion, and Wiser’s preview portion corresponds to the present invention’s “another portion of the content”:

Office Action’s Asserted Correspondence

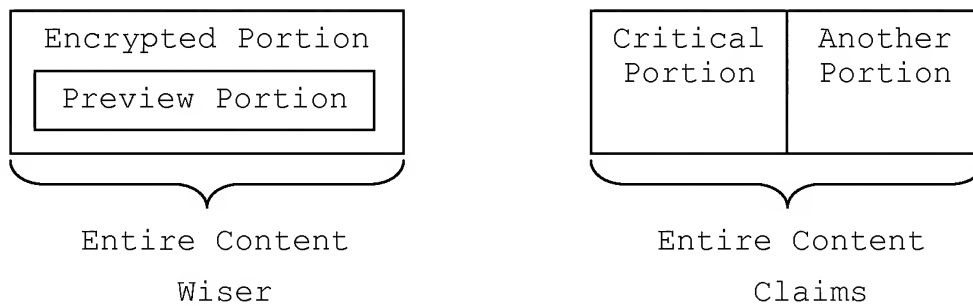
<u>Wiser</u>		<u>Claims</u>
encrypted content	↔	critical portion
preview portion	↔	another portion

But Wiser’s encrypted content is not a “portion” of Wiser’s content; it is the entire content. Consumers can preview part of a song, but they purchase the entire song. Wiser, col. 3 lines 55-61.

In the present specification, three quantities of content are discussed: a critical portion, another portion, and the content as a whole, which is the sum of the critical portion and the “another portion.” [0084, 0100, 0104]. In Wiser, however, only two of these quantities are present. The preview is indeed partial, a “portion”, and is described as such; e.g., Wiser col. 2 lines 13-18, col. 3 lines 54-61, col. 7 lines 60-62. But the “encrypted portion” is not actually a portion – it is the whole of the content. Ibid.

Indeed, the term “encrypted portion” does not appear in Wiser, and it does not appear in the present application (it merely mimics the application’s term “critical portion”). Instead, the term “encrypted portion” was coined for use in the Office Action.

In other words, the Office Action asserts that the following are equal, when they clearly are not:



This mistaken interpretation is reinforced by the Office Action admission at page 2 that the preview portion is “non-important”. The preview is indeed not important, in the sense that it is redundant, because in substance it is merely a part of the encrypted portion. A user would lose no content by omitting the preview and only downloading the encrypted portion. By contrast, the claimed “another portion” is important. It is not merely a subset of the critical portion; it provides additional content. Even when they overlap, a user would lose important content by omitting the “another portion” and only downloading the critical portion. The Office Action’s asserted correspondence is wrong because it fails to recognize this difference in loss of content.

For at least the foregoing reasons, the rejection of these claims under Ground 1 and Section 103 should be reversed.

Ground 1 (Claims 131, 132, 133, 140-145, 147-155): Nuanced Caching Disablement is Missing

The rejections also rely on the art to teach a distinction between allowing disk writes for a predetermined portion of content, and preventing disk writes for another portion of the content. But the references teach only an all-or-nothing approach in which writing all of the content to disk is allowed, or writing none of the content to disk is allowed. The selective caching disablement of the claimed invention is not taught. Caching and other disk write disablement is not tied in the art to critical portions of content, unlike the present claims.

Wiser, for example, discusses caches in some detail, e.g., at col. 22 line 62 to col. 23 line 6. Notably, however, Wiser does not discuss disabling caching, much less disabling caching to prevent copying of specified content portions. If Wiser actually had thought of this functionality and considered it important, it could easily have been discussed along with the other cache-related information. But disabling caching is not even mentioned in Wiser.

Likewise, Benson does not teach a distinction between a critical portion of the content, which is not saved to disk, and another portion of the content, which is saved to disk. Benson's approach is all-or-nothing: the protected program can either write to disk or it cannot. The claimed invention, by contrast, is finer-grained: at least one critical portion is not written to disk, but the rest of the content can be written to disk. This distinction between a portion of content that cannot be saved to disk and another portion that can, is not taught by the cited references.

Although Douglass discusses disabling of caching, the cited language in Douglass again teaches an all-or-nothing approach, in which a disk cache is completely disabled, forcing each request to be passed onward. Thus, the nuanced approach of the claimed invention – in which copies of a critical portion of content are prevented by disallowing caching and other disk writes but caching of “another portion” is allowed – is not taught.

At most, the references take an all-or-nothing approach to disabling caching. More often, they show a complete lack of any concern with caching disablement. Accordingly, the claimed invention's nuanced approach would not have been obvious.

Ground 2 (Claims 134-139, 146): Section 103 is Satisfied

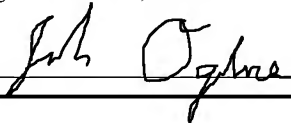
The addition of Salesky does not fix the flaws noted above in discussing Ground 1. Adding Salesky as a reference does not correct the erroneous and unreasonable interpretation of the term “portion”. Nor does Salesky teach a distinction between allowing disk writes for a predetermined portion of content, and preventing disk writes for another portion of the content. Accordingly, the rejections under Ground 2 and Section 103 should also be reversed.

Conclusion

For at least the reasons explained above, the rejections should all be reversed.

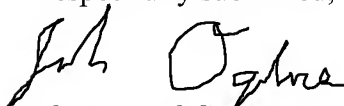
CERTIFICATE OF TRANSMISSION

I hereby certify that this Appeal Brief is being submitted to the Commissioner for Patents through EFS-WEB, on November 9, 2010.



\\pm6-AppealBrief-5045-2-1D

Respectfully submitted,



JOHN W. OGILVIE

Registration No. 37,987

OGILVIE LAW FIRM

2552 Wilshire Circle

Salt Lake City, Utah 84109

801-706-2546 (voice)

801-583-0393 (fax)

Claims Appendix

1 – 130 (canceled)

131. A method for managing content in a shared use operating environment, the shared use operating environment including a registration server, a content server connectable by a network link to the registration server, and a client workstation connectable by a client-server network communications link to the content server, the method comprising the steps of:

registering a user at the registration server, thereby characterizing the user as a registered user;

receiving at the content server a request by the registered user for access to content which contains at least one previously treated critical portion;

authenticating the request;

serving at least the critical portion over the client-server network communications link for presentation to the registered user at the client workstation;

preventing a copy of the critical portion of the content from being created on nonvolatile storage at the client workstation at least in part by disabling caching and other disk writes, and

sending another portion of the content to nonvolatile storage at the client workstation.

132. A method for managing content in an operating environment that includes peer-to-peer nodes, the method comprising the steps of:

registering users;

checking user passwords to prevent unregistered users from receiving content services;

receiving at a first peer node a request by a registered user for access to content which contains at least one previously treated critical portion;

serving at least the critical portion over a network communications link to a second peer node for presentation to the registered user;

preventing a copy of the critical portion of the content from being created on nonvolatile storage at the second peer node, at least in part by disabling caching and other disk writes, and
sending another portion of the content to nonvolatile storage at the second peer node.

133. The method of claim 132, wherein the serving step serves digital content that contains at least one musical recording.

134. The method of claim 132, wherein the serving step serves digital content that contains visual images.

135. The method of claim 132, wherein the serving step serves video content.

136. The method of claim 132, wherein the method delivers content by synchronous sharing.

137. The method of claim 136, wherein the method comprises video conferencing.

138. The method of claim 132, wherein the method delivers content in a real-time manner.

139. The method of claim 132, wherein the method delivers content in an interactive manner.

140. The method of claim 132, wherein the critical portion comprises encrypted content.

141. The method of claim 132, wherein the critical portion comprises compressed content.

142. The method of claim 132, wherein the critical portion comprises licensed content.

143. The method of claim 132, wherein the critical portion comprises content that is compressed and encrypted.

144. The method of claim 132, further comprising the step of disabling use of at least a portion of the content after an expected periodic security handshake is not received.

145. The method of claim 132, further comprising the step of downloading at least a non-critical portion of the content to the second peer node at least one hour before the serving step serves the critical portion.

146. The method of claim 132, wherein the method moves content between peer nodes in response to anticipated requests from users.

147. The method of claim 132, wherein the method moves content between peer nodes in response to actual requests from users.

148. The method of claim 132, wherein the method operates in conjunction with a license enforcement software program executing on the second peer node.

149. The method of claim 132, wherein the method tracks content use in order to create records on which invoices are at least partially based.

150. The method of claim 132, wherein the method tracks content location and determines whether content is already resident on the second peer node or near the second peer node.

151. The method of claim 132, wherein only authenticated network users are able to access the content.

152. The method of claim 131, further comprising reserving a particular piece of courseware content for a particular registered user.

153. The method of claim 131, further comprising monitoring the client-server network communications link so that the user pays only for actual use of the content.

154. The method of claim 131, further comprising downloading at least one non-critical portion of the content to the client workstation at least two hours before serving the critical portion.

155. The method of claim 131, further comprising presenting the registered user with an invoice for usage of the content.

Evidence Appendix

(none)

Related Proceedings Appendix
(none)